Deutscher Bundestag **Drucksache 18/9858**

18. Wahlperiode 29.09.2016

Antwort

der Bundesregierung

auf die Kleine Anfrage der Abgeordneten Dr. Konstantin von Notz, Luise Amtsberg, Volker Beck (Köln), weiterer Abgeordneter und der Fraktion BÜNDNIS 90/DIE GRÜNEN
– Drucksache 18/9616 –

Im Internet offen abrufbare NSA-Hackingwerkzeuge

Vorbemerkung der Fragesteller

Im Verlauf des 13./14. August 2016 wurden überraschend auf der Software-Tauschplattform GitHub 300 Megabyte anspruchsvolle Programme angeboten, mit denen unter anderem das gezielte Hacking von weit verbreiteten kommerziellen Firewalls von Anbietern wie CISCO und Fortinet, von Routern, Betriebssysteme etc. möglich sein soll. Bei den erkennbar nur einen Teil eines Gesamtbestandes darstellenden Programmen soll es sich um Entwicklungen der der NSA-Elitehackergruppe TAO zugeordneten Equation Group handeln, deren Echtheit und Funktionsfähigkeit inzwischen von Experten allgemein bestätigt wird (vgl. „Hacker erbeuteten offenbar NSA-Software“, SPIEGEL ONLINE vom 17. August 2016). Zu der Veröffentlichung der zwischenzeitlich am ursprünglichen Ort nicht mehr verfügbaren, aber vielfach an anderer Stelle gespiegelten Dokumenten und Programmen bekannte sich eine Gruppe mit Namen Shadow Brokers. Während zunächst spekuliert wurde, ob die NSA selbst gehackt worden sein könnte, schätzen einige Experten die angebotenen Programme mittlerweile als das Leak eines Insiders ein, so dass die Möglichkeit diskutiert wird, ob nach Edward Snowden eine weitere Person aus dem weiten Beschäftigtenkreis der NSA gezielt Informationen an die Öffentlichkeit gegeben haben könnte (vgl. beispielsweise Erich Möchel „Der aktuelle NSA-„Hack“ war ein Insiderjob, abrufbar unter http://fm4.orf.at/stories/1772666/).

Nach Angaben unabhängiger Experten stellen die offenbar unter NSA-internen Codenamen veröffentlichten Hacking-Werkzeuge wie Epicbanana, Buzzdirection und Egregiousblunder eine reale und ernstzunehmende Bedrohung für die Sicherheit von Regierungs- und Unternehmensnetzwerken weltweit dar (vgl. Ellen Nakashima „Powerful NSA hacking tools have been revealed online, abrufbar unter www.washingtonpost.com/world/national-security/powerful-nsa-hacking-tools-have-been-revealed-online/2016/08/16/bce4f974-63c7-11e6-96c0-37533479f3f5_story.html).

Die Plattform WikiLeaks hatte in der Zwischenzeit angekündigt, über eine eigene Kopie des veröffentlichten Pakets von Hacking-Werkzeugen zu verfügen, welches ebenfalls zu gegebener Zeit veröffentlicht werden soll. Bisher hat diese Veröffentlichung jedoch noch nicht stattgefunden.

Die Antwort wurde namens der Bundesregierung mit Schreiben des Bundesministeriums des Innern vom 26. September 2016 übermittelt.

Die Drucksache enthält zusätzlich – in kleinerer Schrifttype – den Fragetext.

1. Wann hat die Bundesregierung (einschließlich die ihr nachgeordneten Behörden) erstmalig von der Veröffentlichung der Hacking-Werkzeuge Kenntnis erhalten?

Eine erste Kenntnisnahme erfolgte zwischen dem 13. und 15. August 2016.

2. Wie bewertet die Bundesregierung die Echtheit der angebotenen Hacking-Werkzeuge, und worauf stützt sich ihr Urteil?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat die „frei verfügbaren Hacking-Werkzeuge“ auf technische Plausibilität geprüft und kam zu dem Schluss, dass es sich um funktionierende und bisher teilweise nicht bekannte Werkzeuge handele.

3. In welchem Umfang waren bzw. sind bundesdeutsche Behörden und Unternehmen von den offengelegten Schwachstellen, beispielsweise von CISCO- und Fortinet Netzwerktechnik (siehe hierzu im Einzelnen http://blogs.cisco.com/security/shadow-brokers), betroffen (bitte nach Behörden bzw. Ministerien je gesondert ausführen), und wurden zwischenzeitlich die erforderlichen Gegenmaßnahmen getroffen?

In den Regierungsnetzen sind die betroffenen Komponenten nicht im Einsatz. Bundesdeutsche Behörden und Unternehmen wurden durch das BSI gewarnt. Über die Umsetzung der erforderlichen Gegenmaßnahmen liegen dem BSI keine Erkenntnisse vor.

4. Was wurde von der Bundesregierung bzw. den zuständigen Bundesbehörden wann veranlasst, um etwaigen Schaden von Regierungs- als auch Unternehmensnetzwerken der Bundesrepublik Deutschland abzuwenden?

Das BSI hat Warnungen mit Handlungsempfehlungen an Bundesbehörden, Betreiber Kritischer Infrastrukturen und Mitglieder der Allianz für Cyber-Sicherheit versandt und diese Warnungen mehrfach aktualisiert.

5. Wie bewertet die Bundesregierung die Frage, ob es sich um ein Hack einer der NSA nahestehenden bzw. der NSA zugehörigen Gruppe (z. B. der sogenannten Equation Group) oder die Veröffentlichung eines möglichen NSA-Beschäftigten selbst handeln könnte, und welche Erkenntnisse liegen ihr (oder ihr nachgeordnete Behörden) hierzu vor?

6. Wie bewertet die Bundesregierung die Frage, ob es sich um ein Hack einer der russischen Regierung nahestehenden Gruppe handeln könnte, und welche Erkenntnisse liegen ihr (oder ihr nachgeordnete Behörden) hierzu vor?

Die Fragen 5 und 6 werden gemeinsam beantwortet.

Es liegen keine Erkenntnisse im Sinne der Frage vor.

7. Hat die Bundesregierung (oder ihr nachgeordnete Behörden) Kenntnisse bezüglich der Frage, von wann die entwendete Software ist, und ob die entsprechenden Sicherheitslücken mittlerweile geschlossen wurden?

   Wenn ja, welche Sicherheitslücken wurden zwischenzeitlich geschlossen, und welche bestehen weiterhin?

Keine der Dateien trug einen Zeitstempel nach Juni 2013, jedoch lassen sich Zeitstempel von Dateien ohne großen Aufwand manipulieren. Konkrete Erkenntnisse zu Zeitpunkt der Erstellung der Software liegen der Bundesregierung nicht vor.

Die Schließung der Schwachstellen gestaltet sich wie folgt:

- Die CLI Schwachstelle (CVE-2016-6367) wurde von Cisco im Jahr 2011 geschlossen;
- die EPICBANANAS CLI Schwachstelle (CVE-2016-6367) wurde 2013 von Cisco geschlossen;
- die EXTRABACON SNMP Schwachstelle (CVE-2016-6366) wurde am 16. August 2016 von Cisco geschlossen;
- die BENIGNCERTAIN IKE-Schwachstelle betraf PIX Firewalls mit Versionen <= 6.x. Die PIX-Serie wurde von Cisco im Jahr 2008 abgekündigt;
- die vermutlich unter EGREGIOUSBLUNDER laufende FortiGate Firmware (FOS) Schwachstelle betraf nach Angaben des Herstellers alle vor August 2012 veröffentlichten Versionen von FortiOS;
- die WatchGuard-Schwachstelle hat nach Aussage des Herstellers ausschließlich in älteren RapidStream Geräten existiert. WatchGuard Firebox und XTM Systeme sind demnach nicht verwundbar.

Hinter ELIGIBLECANDIDATE, ELIGIBLEBOMBSHELL, ELIGIBLECONTESTANT und ELIGIBLEBACHELOR verbergen sich allem Anschein nach unterschiedliche Exploits für Firewalls des chinesischen Herstellers TopSec. Seitens TopSec wurden nach BSI-Kenntnis bisher keine Patches veröffentlicht.

Bei BANANAGLEE, FEDTHROUGH und ZESTYLEAK handelt es sich um für NetScreen-Firewalls des Herstellers Juniper Networks nutzbare Implantate. In einem Blog-Post[2] bestätigt Juniper grundsätzlich die Existenz von Implantaten für NetScreen Systeme. In Reaktion wird auf Prüfverfahren verwiesen, mit denen sich modifizierte Firmware-Images erkennen lassen.

8. Hat die Bundesregierung (oder ihr nachgeordnete Behörden) Kenntnisse bezüglich der Frage, ob es sich um einen gezielten Hack oder eventuell eher um einen „Zufallsfund“ auf einem von der „Equation Group“ oder anderen Gruppe verwendeten Command-and-Control-Server handelt?

   Wenn ja, welche?

9. Welche Erkenntnisse hat die Bundesregierung (oder ihr nachgeordnete Behörden) zu Verbindungen von den nun veröffentlichten Dokumenten und den Dokumenten aus dem Umfeld Edward Snowdens, und welche Rückschlüsse lassen diese Erkenntnisse aus Sicht der Bundesregierung auf die jeweilige Echtheit der veröffentlichten Dokumente zu?

Die Fragen 8 und 9 werden gemeinsam beantwortet.

Hierzu liegen keine Erkenntnisse vor.

10. Unabhängig von der Frage der Herkunft und Verantwortung für die Erstellung der Hacking-Werkzeuge, hält die Bundesregierung es für die Aufgabe auch bundesdeutscher Behörden (etwa die geplante ZITIS), kommerzielle Netzwerkelemente wie beispielsweise die betroffenen, weithin im Einsatz befindlichen CISCO- und und Fortinet-Produkte, Firewall-Programme, Router, Betriebssysteme etc. gezielt auf Schwachstellen zu analysieren und für den Angriff auf Netzwerke derartige Instrumente und das Wissen über Schwachstellen vorzuhalten?

Die Bundesregierung nutzt bereits jetzt die ihr zur Verfügung stehenden Ressourcen, um die IT-Sicherheit Deutschlands möglichst umfassend zu gewährleisten. Zu diesem Zweck werden bereits heute wichtige Hard- und Software-Komponenten auf mögliche technische Schwachstellen untersucht und kritische Infrastrukturen zum Schutze des Landes entsprechend gesichert.

11. Teilt die Bundesregierung, auch angesichts der jetzigen Veröffentlichungen, die Ansicht der Fragesteller, dass es dringend angeraten ist, Schwachstellen, sobald sie bekannt sind, statt sie bewusst offen zu halten, um sie ggf. zu einem späteren Zeitpunkt nutzen zu können, umgehend zu schließen, auch, um zu verhindern, dass diese Dritten offenstehen und ggf. missbraucht werden können?

Die Bundesregierung steht für eine sichere IT-Infrastruktur und spricht sich vor dem Hintergrund einer möglichen missbräuchlichen Verwendung gegen das Offenhalten von Sicherheitslücken aus. In diesem Sinn verfolgt z. B. das BSI eine Responsible-Disclosure-Politik und geht aktiv auf Hersteller zu, damit diese gemeldete Schwachstellen schließen können.

12. Wird sich die Bundesregierung, wie dies beispielsweise in einem Entschließungsantrag der fragestellenden Fraktion zu der dritten Beratung des Gesetzentwurfs der Bundesregierung eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) auf Bundestagsdrucksache 18/5127 im Juni 2015 forderte, für eine grundsätzliche Pflicht zur unverzüglichen Veröffentlichung von Wissen über Sicherheitslücken einsetzen?

Gemäß § 7a Absatz 1 Satz 1 des BSI-Gesetzes kann das BSI zur Erfüllung seiner Aufgaben nach § 3 Absatz 1 Satz 2 Nummer 1, 14 und 17 auf dem Markt bereitgestellte oder zur Bereitstellung auf dem Markt vorgesehene informationstechnische Produkte und Systeme untersuchen. § 7 Absatz 2 des BSI-Gesetzes enthält eine eindeutige Zweckbindung und stellt klar, dass die aus den Untersuchungen gewonnenen Erkenntnisse ausschließlich zur Erfüllung dieser Aufgaben genutzt werden dürfen. Das BSI darf seine Erkenntnisse weitergeben und veröffentlichen, soweit dies zur Erfüllung dieser Aufgaben erforderlich ist. Zuvor ist dem Hersteller der betroffenen Produkte und Systeme mit angemessener Frist Gelegenheit zur Stellungnahme zu geben.

Die Bundesregierung sieht an der bestehenden Regelung keinen Änderungsbedarf. Die mit dem IT-Sicherheitsgesetz in § 7a des BSI-Gesetzes eingefügte Regelung zur Untersuchung von informationstechnischen Produkten und Systemen ist sachgerecht. Sofern der Hersteller – etwa bei einer festgestellten Sicherheitslücke – selbst an die Öffentlichkeit geht oder sonst Abhilfe schafft, ist eine zusätzliche Veröffentlichung der Erkenntnisse durch das BSI nicht erforderlich.

Eine grundsätzliche Verpflichtung des BSI zur unverzüglichen Veröffentlichung wäre demgegenüber nicht nur rechtlich problematisch, sondern auch im Ergebnis nicht zielführend, etwa dann nicht, wenn die Sicherheitslücke weder geschlossen werden kann noch alternative Produkte zur Verfügung stehen. Eine Veröffentlichung würde in diesem Fall nur potentiellen Angreifern helfen, eine bestehende Sicherheitslücke auszunutzen.

13. Wird die Bundesregierung, wie dies in der in Frage 12 Erwähnung findenden Initiative gefordert wird, dafür Sorge tragen, dass, auch um eine Beförderung des Schwarzmarktes für Sicherheitslücken, welche die Integrität digitaler Infrastrukturen gefährden, der staatliche Aufkauf und die Zurückhaltung bzw. Nichtveröffentlichung von Wissen über Sicherheitslücken, gesetzlich verboten wird?

    Wenn ja, wann ist mit der Vorlage zu rechnen?

    Falls nein, warum nicht?

Die Strafverfolgungsbehörden des Bundes und der Länder gehen im Rahmen der geltenden Rechtslage und ihrer jeweiligen Zuständigkeiten gezielt gegen organisiertes Verbrechen, Cybercrime und Terrorismus vor.

Die Strafverfolgung richtet sich dabei auch konsequent gegen strafbare Handlungen und Inhalte des Schwarzmarktes. Die gesetzlichen Regelungen sind dabei bereits heute umfassend.

14. Sieht die Bundesregierung den Ankauf und die Zurückhaltung bzw. Nichtveröffentlichung von Wissen über Sicherheitslücken durch staatliche Stellen als vereinbar mit ihrem Ziel, die IT-Sicherheit zu erhöhen, an oder teilt die Bundesregierung die Ansicht der Fragesteller, dass beides nicht miteinander in Einklang zu bringen ist?

Erkenntnisse zu Sicherheitslücken, die öffentlich bekannt sind, auf eigenen Analysen beruhen oder beispielsweise im Rahmen der Zusammenarbeit von CERTs gewonnen werden, diskutiert das BSI gemäß seines gesetzlichen Auftrages regelmäßig mit den betroffenen Herstellern. Das Ziel ist hierbei, dass die Hersteller diese Sicherheitslücken kurzfristig schließen können.

15. Verfügt die Bundesregierung oder ihr nachgeordnete Behörden inzwischen über Kopien der online angebotenen Hacking-Werkzeuge, und wenn nein, auf welche Weise wurde Vorsorge getroffen (etwa durch Ansprache anderer betroffener Staaten; Kontakt mit den USA, der NSA etc.), dass diese Werkzeuge nicht gegen Stellen in und gegen Institutionen der Bundesrepublik Deutschland eingesetzt werden können?

Der Bundesnachrichtendienst (BND) und das BSI verfügen über die „frei verfügbaren Dateien."

16. Sind Regierungsstellen bzw. Teile von Regierungsnetzwerken von den von CISCO benannten Sicherheitslücken (Exploits) oder anderen Schwachstellen, z. B. für die Umgehung von gängigen Firewall-Programmen, zur Infiltrierung von Routern und/oder Betriebssystemen, betroffen, wenn ja, in welchem bezifferbaren Umfang, und konnten diese Lücken inzwischen geschlossen werden?

In Regierungsnetzen sind die betroffenen Komponenten nicht im Einsatz.

17. Wurde zwischenzeitlich der zur Koordination mit der Wirtschaft geschaffene Cybersicherheitsrat mit diesem Vorfall befasst, und wenn ja, wann, und mit welcher Zielrichtung?

Die letzte Sitzung des Cyber-Sicherheitsrates fand am 8. Juli 2016 statt. Die in Rede stehende Veröffentlichung erfolgte am 13. August 2016. Der Cyber-Sicherheitsrat hat sich bisher nicht mit diesem Vorfall befasst.

18. Wann war das Bundesamt für Sicherheit in der Informationstechnik (BSI) erstmalig mit diesem Vorgang befasst, und was hat es hierzu zwischenzeitlich veranlasst?

Auf die Antworten zu den Fragen 1, 2, 4, 15 und 17 wird verwiesen.

19. Gibt der Vorfall der Bundesregierung Anlass, ihre Bewertung der Vorteile und Risiken der Neugründung der sogenannten ZITIS-Behörde zu überdenken, welche selbst zum ausgewählten Ziel von Angriffen werden dürfte, die bei Erfolg gravierende Risiken für die nationalen Kommunikationsinfrastrukturen als auch für die Betriebs- und Geschäftsgeheimnisse von Unternehmen der Wirtschaft nach sich ziehen?

ZITiS wird sehr strengen personellen und materiellen Sicherheitsregeln unterliegen, die im Besonderen auf die IT-Infrastruktur Anwendung findet. Die neue Behörde wird sich damit in die Sicherheitsstandards von BKA (Bundeskriminalamt), BPOL (Bundespolizei), BfV (Bundesamt für Verfassungsschutz), BND und BSI einreihen. Ferner werden auch für ZITiS die Grundsätze der Verschlusssachenanweisung (VSA) gelten, durch die zusätzliche hohe Standards für die Verwahrung schützenswerter Erkenntnisse festgeschrieben sind.



Satz: Satzweiss.com Print, Web, Software GmbH, Mainzer Straße 116, 66121 Saarbrücken, www.satzweiss.com
Druck: Printsystem GmbH, Schafwäsche 1-3, 71296 Heimsheim, www.printsystem.de
Vertrieb: Bundesanzeiger Verlag GmbH, Postfach 10 05 34, 50445 Köln, Telefon (02 21) 97 66 83 40, Fax (02 21) 97 66 83 44, www.betrifft-gesetze.de
ISSN 0722-8333